ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0025—2023
代替 GM/T 0025—2014

SSL VPN 网关产品规范

SSL VPN gateway product specification

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GM/T 0025—2014《SSL VPN 网关产品规范》，与 GM/T 0025—2014 相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了 GB/T 25069（见第 2 章）、GM/T 0016（见 6.3.1）、GM/T 0028（见 6.3.2.2，6.3.2.3 和 6.3.2.4）、GM/T 0050（见 6.4.1）、GM/T 0062（见 6.4.2.3.3）和 GM/Z 4001（见第 2 章），删除了 GB/T 17964 和 GM/T 0014（见 2014 年版的第 2 章）；

b) 删除了术语“密码算法”（见 2014 年版的 3.1.1）、“密码杂凑算法”（见 2014 年版的 3.1.2）、“非对称密码算法/公钥密码算法”（见 2014 年版的 3.1.3）、“对称密码算法”（见 2014 年版的 3.1.4）、“分组密码算法”（见 2014 年版的 3.1.5）、“密文分组链接工作模式”（见 2014 年版的 3.1.6）、“初始化向量/值”（见 2014 年版的 3.1.7）、“数字证书”（见 2014 年版的 3.1.8）、“SSL 协议”（见 2014 年版的 3.1.9）、“虚拟专用网络”（见 2014 年版的 3.1.10）和“SM2 算法”（见 2014 年版的 3.1.11）；

c) 增加了缩略语“GCM”和“TLCP”（见第 4 章）；

d) 增加了 GCM 模式（见 5.1）；

e) 增加了对随机数生成的描述（见 6.1.1）；

f) 更改了产品性能参数要求的描述（见 6.2，2014 年版的 5.2）；

g) 更改了密钥安全的描述（见 6.3.1，2014 年版的 5.3.1）；

h) 增加了敏感参数配置安全（见 6.3.2.2）；

i) 增加了应符合 GM/T 0028 对硬件模块物理安全规定的描述（见 6.3.2.3）；

j) 增加了应符合 GM/T 0028 对软件/固件安全的规定和软件升级相关要求的描述（见 6.3.2.4）；

k) 增加了远程管理（见 6.4.1）；

l) 增加了一些管理员口令量化的指标（见 6.4.2.2）；

m) 增加了设备管理中注册和监控（6.4.2.3.2）；

n) 更改了“随机数发生器”的要求（见 6.5.3，2014 年版的 5.4.4.3）；

o) 更改了“加密部件”的描述（6.5.2，2014 年版的 5.4.4.2）；

p) 增加了“检测说明”“外观和结构检查”和“提交文档的检查”（见 7.1，7.2 和 7.3）；

q) 增加了安全管理检测的检测方法的描述（见 7.6）；

r) 增加了敏感参数配置安全检测的描述（见 7.6.1.3）；

s) 增加了远程管理检测的描述（见 7.6.2.4）；

t) 增加了硬件要求的检测方法的描述（见 7.7）；

u) 更改了判定规则（见第 8 章，2014 年版的第 7 章）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：格尔软件股份有限公司、无锡江南信息安全工程技术中心、山东得安信息技术有限公司、北京信安世纪科技股份有限公司、飞天诚信股份有限公司、广东省电子商务认证有限公司、北京国脉信安科技有限公司、中电信量子信息科技集团有限公司、山东渔翁信息技术股份有限公司、天融

信科技集团股份有限公司、上海数字证书认证中心有限公司、智巡密码(上海)检测技术有限公司、山东大学、兴唐通信科技有限公司、中电科网络安全科技股份有限公司、北京数字认证股份有限公司。

本文件主要起草人:郑强、谭武征、孔凡玉、胡金山、李元正、汪宗斌、朱鹏飞、梁宁宁、药乐、王鹏、罗俊、安高峰、刘承、韩玮、李述胜、王丽娜、邱媛、韩琳、董明富。

本文件所代替文件的历次版本发布情况为:

——2014 年首次发布为 GM/T 0025—2014;

——本次为第一次修订。

SSL VPN 网关产品规范

1 范围

本文件规定了 SSL VPN 网关产品的功能要求、硬件要求、软件要求、安全性要求和检测要求。

本文件适用于 SSL VPN 网关产品的研发、检测和管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 9813.3 计算机通用规范 第 3 部分：服务器

GB/T 15153.1 远动设备及系统 第 2 部分：工作条件 第 1 篇：电源和电磁兼容性

GB/T 25069 信息安全技术 术语

GM/T 0005 随机性检测规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0024 SSL VPN 技术规范

GM/T 0028 密码模块安全技术要求

GM/T 0050 密码设备管理 设备管理技术规范

GM/T 0062 密码产品随机数检测要求

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069 和 GM/Z 4001 界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

CBC：密码分组链接(Cipher Block Chaining)

GCM：Galois 计数器模式(Galois Counter Mode)

SSL：安全套接层协议(Secure Sockets Layer)

TLCP：传输层密码协议(Transport Layer Cryptography Protocol)

VPN：虚拟专用网络(Virtual Private Network)

5 密码算法和密钥种类

5.1 算法要求

SSL VPN 使用的非对称密码算法、对称密码算法、密码杂凑算法和随机数生成算法应符合密码国家标准、行业标准的相关要求。算法及使用方法如下。

a) 非对称密码算法用于认证、数字签名和数字信封。

b) 对称密码算法使用分组密码算法，用于密钥交换数据的加密保护和报文数据的加密保护。算法的工作模式为 GCM 模式或 CBC 模式。

c) 密码杂凑算法用于对称密钥生成、完整性校验和数字签名。

d) 生成的随机数应符合 GM/T 0005 的检测要求。

5.2 密钥种类

5.2.1 预主密钥

预主密钥(pre_master_secret)是双方协商生成的密钥素材，用于生成主密钥。

5.2.2 主密钥

主密钥(master_secret)是由预主密钥、客户端随机数、服务端随机数、常量字符串，经计算生成的密钥素材，用于生成工作密钥。

5.2.3 工作密钥

工作密钥包括数据加密密钥和校验密钥。其中数据加密密钥用于数据的加密和解密，校验密钥用于数据的完整性计算和校验。在本文件中，发送方使用的工作密钥称为写密钥，接收方使用的工作密钥称为读密钥。

5.2.4 服务端密钥

服务端密钥为非对称密码算法的密钥对，包括签名密钥对和加密密钥对，用于握手过程中服务端身份鉴别和预主密钥的协商。其中基于证书体系的非对称算法的密钥对，其签名密钥对由 VPN 自身密码模块产生，加密密钥对应通过 CA 认证中心向 KMC 申请。

5.2.5 客户端密钥

客户端密钥为非对称密码算法的密钥对，包括签名密钥对和加密密钥对，用于握手过程中客户端身份鉴别和预主密钥的协商。其中基于证书体系的非对称算法的密钥对，其签名密钥对由对应的客户端密码模块产生(例如智能密码钥匙)，加密密钥对应通过 CA 认证中心向 KMC 申请。

6 SSL VPN 网关产品要求

6.1 产品功能要求

6.1.1 随机数生成

SSL VPN 网关应具备独立的随机数生成功能。

6.1.2 工作模式

SSL VPN 网关产品工作模式分为客户端－服务端模式和网关－网关模式两种。其中客户端－服务端模式是必备模式，网关－网关模式是可选模式。

6.1.3 密钥交换

SSL VPN 网关产品应具有密钥交换功能，通过协商产生工作密钥。

密钥交换应符合 GM/T 0024 的要求。

6.1.4 安全报文传输

SSL VPN 网关产品具有安全报文传输功能，保证数据的安全传输。

6.1.5 身份鉴别

SSL VPN 网关产品应具有实体鉴别的功能，鉴别方式采用数字证书或基于标识算法的鉴别机制。数字证书格式应符合 GM/T 0015。服务端的鉴别是必备功能，客户端的鉴别是可选功能，应支持基于数字证书或者基于标识算法的鉴别机制。任何一种鉴别方式都应保证鉴别的完整性和有效性。

6.1.6 访问控制

SSL VPN 网关产品应具有细粒度的访问控制功能，基于用户或用户组对资源进行有效控制。其中对网络访问至少应控制到 IP 地址、端口和协议，对 Web 资源的访问至少应控制到 URL，并能根据访问时间进行控制。

6.1.7 密钥更新

SSL VPN 网关产品应具有根据时间周期或报文流量进行工作密钥更新的功能。其中，根据时间周期进行更新为必备功能，根据报文流量进行更新为可选功能。对于客户端－服务端模式，工作密钥的最长更新周期不超过 8 h，对于网关－网关模式，工作密钥最长时间更新周期不超过 1 h。

6.1.8 信息审计

SSL VPN 网关产品应具有信息审计功能，能对用户对系统的访问进行详细记录，记录信息包括：时间、用户 IP、用户证书信息、访问资源、上传流量、下载流量、访问结果、错误原因。

6.1.9 信息传递

SSL VPN 网关应具有信息传递功能，用户访问 HTTP 应用时，系统在完成相应的身份鉴别后，把验证结果、用户的基本信息插入到 HTTP 请求中传送给后台的应用系统，应用系统通过标准的 HTTP 操作即可获取信息，并基于该信息作相应的访问控制以及进行相应的业务审计。获取的信息包括：用户 IP 地址，用户证书的关键信息。

6.1.10 客户端主机安全检查

SSL VPN 网关产品应具有客户端主机安全检查功能。客户端在连接服务端时，根据服务端下发的客户端安全策略检查用户操作系统的安全性。不符合安全策略的用户将无法使用 SSL VPN。

客户端安全策略应至少包括以下条件之一：

a) 已安装并启用反病毒软件；

b) 已安装并启用个人防火墙；
c) 已安装最新的操作系统安全补丁；
d) 已为系统设置了登录口令。

6.2 产品性能参数

6.2.1 最大并发用户数

同时在线用户的最大数目，产品应满足用户网络环境对最大并发用户数量性能的要求。

6.2.2 最大并发连接数

同时在线 TLCP 连接的最大数目，产品应满足用户网络环境对最大 TLCP 连接数量性能的要求。

6.2.3 每秒新建连接数

每秒钟可新建的最大 TLCP 连接数目，产品应满足用户网络环境对每秒能接入新 TLCP 连接性能的要求。

6.2.4 加解密吞吐率

在丢包率为 0 的条件下，产品应满足用户网络环境对网络数据加解密吞吐性能的要求。

6.3 产品安全性要求

6.3.1 密钥安全

加密密钥对由外部密钥管理机构产生并由外部认证机构签发加密证书。加密密钥对的私钥保护方法应符合 GM/T 0016。

签名证书、加密证书和加密密钥对的私钥应能被导入 SSL VPN 网关产品中。

在 SSL VPN 网关产品中，密钥的私钥应有安全保护措施。

密钥应按设定的安全策略进行更新。

密钥可以安全形式进行备份，并在需要时能恢复。

工作密钥产生后应保存在易失性存储器中，达到其更新条件后应立即更换，在连接断开、设备断电时应销毁。

6.3.2 配置安全

6.3.2.1 数据配置安全

所有的配置数据应保证其在设备中的完整性、可靠性。应有管理界面对配置数据进行配置和管理，管理员进入管理界面应通过身份鉴别。

6.3.2.2 敏感参数配置安全

包括密钥在内的敏感安全参数的生成、建立、输入、输出、存储和置零的全生命周期的管理应符合 GM/T 0028 的要求。

6.3.2.3 硬件安全

SSL VPN 网关产品硬件应符合 GM/T 0028 对硬件模块物理安全的规定。

SSL VPN 网关产品应提供安全措施，保证密码算法、密钥、关键数据的存储安全。

所有密码运算应在独立的密码部件中进行。

除必需的通信接口和管理接口以外，不提供任何可供调试、跟踪的外部接口。内部的调试、检测接口应在产品定型后封闭。

6.3.2.4 软件安全

SSL VPN 网关产品的软件或固件应符合 GM/T 0028 对软件/固件安全的规定。

操作系统应进行安全加固，裁减一切不需要的模块，关闭所有不需要的端口和服务。

任何操作指令及其任意组合，不能泄露密钥和敏感信息。

软件升级应具备修复安全漏洞的能力，在升级前应对升级包文件进行完整性校验。

6.3.2.5 客户端安全

SSL VPN 客户端产品应具有完整性的自校验功能，包括厂商对客户端软件的签名，以保护信息的完整性。

6.3.3 管理安全

6.3.3.1 分权管理

应实现系统管理员、安全管理员、系统审计员分权管理。

系统管理员负责对软件环境日常运行的管理和维护，以及对系统的备份和操作系统恢复。

系统审计员负责对系统中的日志进行安全审计。

安全管理员负责业务配置、应用管理、授权管理操作。

6.3.3.2 管理员登录安全

管理员通过数字证书认证进行鉴别，并通过加密通道对 SSL VPN 网关进行管理配置，管理员只能通过被授权的终端登录到 SSL VPN 网关进行相应的配置操作。

6.4 产品管理要求

6.4.1 远程管理

远程管理：SSL VPN 网关产品应提供协议接口接受管理中心通过网络远程对其设备状态、网络配置、安全策略进行查询、监控和管理。对密码设备的管理宜符合 GM/T 0050 的设备管理技术规范。

a） 合规性验证

SSL VPN 网关产品宜提供远程调用接口对 SM2、SM3、SM4 和密钥随机性进行合规性验证，验证协议和接口应符合密码国家标准、行业标准的相关要求。

b） 远程参数配置

SSL VPN 网关产品宜提供协议和接口接受管理中心远程对其参数进行配置。

c） 远程监控

1） 参数查询

SSL VPN 网关产品宜提供协议和接口接受管理中心对其安全策略、安全参数、网络参数、用户参数配置信息和日志进行查询，并可提供分类查询和关键字检索手段。

2） 状态监测

SSL VPN 网关产品宜提供协议和接口接受管理中心远程对其运行状态（CPU、内存和非易失性存储介质系统资源的占有率）、系统信息（开机时间、运行时间、系统时间和设备名

字及 IP)、网络流量、是否在线、隧道状态(建立时间、加密流量、有效期)进行远程实时查询,并在设备状态明显异常时可向管理中心报警。

3) 远程控制

SSL VPN 网关产品宜提供协议和接口接受管理中心远程对其进行重启、故障诊断、各项功能的关闭和启用操作。

4) 时间同步

SSL VPN 网关产品宜提供远程调用接口接受管理中心对其进行远程时间同步。

6.4.2 管理内容

6.4.2.1 日志管理

SSL VPN 网关产品应提供日志记录、查看和导出功能。SSL VPN 网关产品的客户端不要求日志管理。

日志内容包括:

a) 管理员操作行为,包括用户管理、登录认证、系统配置、密钥管理操作;

b) 用户访问行为,包括用户、时间、访问资源、结果;

c) 异常事件,包括认证失败、非法访问异常事件的记录。

日志格式应包括事件发生的日期和时间、主体身份和事件内容。

6.4.2.2 管理员管理

SSL VPN 服务端产品应设置管理员,进行系统配置、密钥生成、导入、备份和恢复操作。管理员应持有表征用户身份信息的硬件装置与登录口令相结合登录系统,进行管理操作前应通过身份鉴别。

登录口令长度应不小于 8 个字符,且至少由数字、字母和特殊字符其中的两种类型组成。

使用错误口令或非法身份登录的次数限制应在半小时内次数小于或等于 8。

6.4.2.3 设备管理

6.4.2.3.1 设备初始化

SSL VPN 网关产品的初始化,除应由厂商进行的操作外,系统配置、密钥的生成和管理、管理员的产生均应由用户完成。

6.4.2.3.2 注册和监控

SSL VPN 网关产品进行远程管理时,应具有向管理中心进行注册的功能,同时接受管理中心对其运行状态的实时监控管理。

6.4.2.3.3 设备自检

SSL VPN 网关产品在开机、管理接口收到管理指令时应进行自检。

应对密码运算部件关键部件进行正确性检查。应确保密码运算部件正常工作,设备所采用的各种密码算法:包括对称、非对称和杂凑算法的正确性在设备自检时应得到验证。

应对存储的密钥敏感信息进行完整性检查。应确保设备密钥得到安全保护,工作密钥和会话密钥不存放在非易失性存储介质中。

应对硬件随机数产生部件进行检查,应确保硬件随机数产生部件正常工作,随机数产生质量符合 GM/T 0005 的规定。

应对身份认证介质及其接口进行检查，确保其正常工作。

应对随机数发生器进行检查，应符合 GM/T 0062 的 E 类。

可对 CPU、内存、网络接口、非易失性存储介质物理部件进行常规检查，确保各关键部件正常工作。

对算法正确性、密钥完整性、随机数可靠性检测为必选项，硬件功能模块、软件功能模块正确性检测为可选项。在检查不通过时应报警并停止工作。

6.5 产品硬件要求

6.5.1 对外接口

SSL VPN 网关产品应分别具有工作网口和管理接口。其中管理接口应包括本地维护接口和远程管理接口，可采用网口或串口通信；工作网口应至少具备两个，分别为内网接口和外网接口。

6.5.2 加密部件

SSL VPN 网关产品应采用通过商用密码检测认证的密码模块或安全芯片作为密码部件实现密码运算和密钥管理。

6.5.3 随机数发生器

SSL VPN 网关采用的随机数发生器应通过商用密码检测认证，生成的随机数应由多路硬件随机源产生并符合 GM/T 0005 的要求，至少采用两个独立的物理噪声源芯片实现。

6.5.4 环境适应性

SSL VPN 网关产品的工作环境应符合 GB/T 9813.3 中关于“气候环境适应性”的规定要求。

6.5.5 电磁兼容性

SSL VPN 网关产品应满足一定条件下的电磁兼容等级，产品应符合 GB/T 15153.1 中指标和严酷等级要求。

6.5.6 可靠性

SSL VPN 网关产品的平均无故障工作时间应不低于 10 000 h。

6.6 过程保护

设置必要保护措施，保障产品在运输和安装过程中的安全，不被嵌入恶意信息。

6.7 参数可配置能力要求

SSL VPN 网关产品可支持对设备的相关参数进行配置，包括网络接口的 MTU(最大传输单元)、MAC 地址、速度(自适应或者固定速率)、双工/半双工、是否开启流控。

7 SSL VPN 网关产品检测要求

7.1 检测说明

检测要求规定了 SSL VPN 网关的通用检测内容和方法。检测应包括外观和结构检查、提交文档的检查、功能检测、性能检测、安全管理检测和硬件检测。

7.2 外观和结构的检查

根据产品的物理参数，对被检测设备的外观、尺寸、内部部件及附件进行检查。

7.3 提交文档的检查

被检测设备研制单位应按照具备资质的商用密码检测、认证机构的检测要求提交相关文档资料，作为 SSL VPN 网关的检测认证依据。

7.4 产品功能检测

7.4.1 工作模式

在客户端－服务端工作模式下，客户端应能通过服务端访问到受保护内网服务器。在网关－网关工作模式下，一个网关保护的客户主机应能访问到另一个网关保护的内网服务器。检测结果应符合 6.1.2 的要求。

7.4.2 随机数功能

对随机数进行检测，检测结果应符合 6.1.1 的要求。

7.4.3 密钥交换

密钥交换协议应按照 GM/T 0024 的要求进行。检测结果应符合 6.1.3 的要求。

7.4.4 安全报文传输

安全报文封装协议应按照 GM/T 0024 的要求进行。检测结果应符合 6.1.4 的要求。

7.4.5 身份鉴别

身份鉴别应按照 GM/T 0024 的要求进行。检测结果应符合 6.1.5 的要求。

7.4.6 访问控制

从客户端访问服务端保护的内网服务器，应只能访问到授权的资源。检测结果应符合 6.1.6 的要求。

7.4.7 密钥更新

密钥更新应按照 GM/T 0024 的要求进行。检测结果应符合 6.1.7 的要求。

7.4.8 信息审计

用户通过访问后，系统应能对用户访问信息进行记录。监测结果应符合 6.1.8 的要求。

7.4.9 信息传递

用户通过 SSL VPN 访问 HTTP 应用时，应用系统可从 HTTP 请求信息中获取用户信息。监测结果应符合 6.1.9 的要求。

7.5 产品性能检测

7.5.1 最大并发用户数

最大并发用户数是指在同一时刻能与服务器进行交互的在线用户的最大数量。这些用户的最大特征是和服务器产生了交互，这种交互既可是单向的传输数据，也可是双向的传送数据。在检测平台模拟多个客户端行为，与服务端建立 TLCP 会话，在这个会话上，从内网服务器下载 512 字节页面的数据，并在内网服务器上设置页面延迟，以保证在整个负载增加的过程中每一个会话均被保持且有数据通过。然后，不断增加客户端，并重复此过程，取负载稳定期的平均并发会话数作为测试结果。

7.5.2 最大并发连接数

最大并发连接数是指在同一时刻能与服务器进行交互的连接的最大数量。在检测平台模拟多个客户端行为，与服务端进行 TLCP 连接并保持，然后不断增加客户端，并重复此过程，直到无法建立并保持连接为止。取已经接入的 TLCP 连接数目为测试结果。

7.5.3 每秒新建连接数

在检测平台模拟多个客户端行为，并发与服务端建立 TLCP 会话。重复此过程一段时间，取每秒建立 SSL 会话数目的平均值作为测试结果。

7.5.4 吞吐率

在检测平台模拟多个客户端行为，与服务端建立 TLCP 会话。在这个会话上，从内网服务器下载 1 MB 数据，重复以上步骤，直到每个用户成功下载 20 MB 大小的数据。然后向内网服务器上传 1 MB 数据，重复以上步骤，直到每个用户成功上传 20 MB 大小的数据。取内网服务器收发数据的平均速率作为测试结果。

7.6 安全管理检测

7.6.1 安全检测

7.6.1.1 密钥检测

对密钥进行管理以确保密钥安全。在被测设备的管理界面上进行设备密钥的产生或导入、备份和恢复以及更新操作。密钥的检测结果应符合 6.3.1 的要求。

7.6.1.2 配置数据安全

所有的配置数据应保证其在设备中的完整性、可靠性。应有管理界面对配置数据进行配置和管理，管理员进入管理界面应通过身份鉴别。检测结果应符合 6.3.2.1 的要求。

7.6.1.3 敏感参数配置安全

对被检测设备的包括密钥在内的敏感安全参数进行生成、建立、输入、输出、存储和置零操作。检测结果应符合 6.3.2.2 的要求。

7.6.1.4 硬件安全

审查厂商提供的设计文档和厂商提交的产品安全性承诺，应符合相应产品规范要求。检测结果应符合 6.3.2.3 的要求。

7.6.1.5 软件安全

使用漏洞扫描工具探测系统的端口和服务，并审查厂商提供的设计文档和厂商提交的产品安全性承诺，应符合相应产品规范的要求。检测结果应符合 6.3.2.4 的要求。

7.6.1.6 客户端安全

SSL VPN 网关的客户端产品应能通过数字签名等技术实现完整性的自校验功能。检测结果应符合 6.3.2.5 的要求。

7.6.1.7 管理安全

7.6.1.7.1 分权管理

系统管理员、安全管理员、系统审计员应具备各自的分权管理职责。检测结果应符合 6.3.3.1 的要求。

7.6.1.7.2 管理员登录安全

管理员应能通过基于数字证书技术的身份鉴别，并通过加密通道对 SSL VPN 网关进行管理配置，管理员应能通过被授权的终端登录到 SSL VPN 网关进行相应的配置操作。检测结果应符合 6.3.3.2 的要求。

7.6.2 安全管理检测

7.6.2.1 日志管理

可以查看并导出日志记录。日志格式应符合相关产品规范的要求。检测结果应符合 6.4.2.1 的要求。

7.6.2.2 管理员管理

用非法的身份或错误的口令登录，系统应拒绝；当连续重试次数到达系统设定的限制值时系统应锁定；用合法的身份和正确口令登录，应能进入管理界面，进行相应的管理操作。检测结果应符合 6.4.2.2 的要求。

7.6.2.3 设备管理

7.6.2.3.1 设备初始化

对设备进行初始化操作，结果应符合相应产品规范的要求。检测结果应符合 6.4.2.3.1 的要求。

7.6.2.3.2 注册和监控

当系统有管理中心时，进行设备的注册、状态监控管理操作，对于异常操作（例如，中断网络连接或停止密码部件工作），被检测设备应发出告警。检测结果应符合 6.4.2.3.2 的要求。

7.6.2.3.3 设备自检

对设备进行自检操作，产品检测结果应符合相应产品规范的要求。检测结果应符合 6.4.2.3.3 的要求。

7.6.2.4 远程管理

如果被检测设备具备远程参数配置或远程监控功能，使用被检测设备提供的接口，对被检测设备进行参数查询、状态检测、远程控制和时间同步的操作。检测结果应符合 6.4.1 的要求。

7.7 硬件检测

7.7.1 外部接口

对被检测设备的外部接口进行检查，检查结果应符合 6.5.1 的要求。

7.7.2 密码部件

对被检测设备的密码部件进行检查，检查结果应符合 6.5.2 的要求。

7.7.3 随机数发生器

对被检测设备的随机数发生器进行检查，检查结果应符合 6.5.3 的要求。

7.7.4 其他硬件

对被检测设备的环境适应性、电磁兼容性和可靠性进行检查，检查结果应符合 6.5.4.～6.5.6 的要求。

8 判定规则

本文件中，7.4、7.6(除 7.6.1.2)和 7.7(除 7.7.4)外的任意一项不合格，判定为产品密码检测不合格。